LIST OF CURRENT CLAIMS

1. (Currently Amended) A method for authenticating a user ~~(U)~~ of a data carrier ~~(C)~~ for authorized use of the data carrier and for authenticating a data carrier terminal ~~(T)~~ for authorized accessing by the data carrier terminal of memory areas of the data carrier, comprising the following steps:

[[-]] reading a secret code ~~(CODE)~~ from the data carrier ~~(C)~~ by the data carrier terminal ~~(T)~~, ~~whereby~~ wherein the secret code ~~(CODE)~~ is stored on a memory location that can be accessed only by authorized data terminals ~~(T)~~ [[and/]]or can be decrypted correctly only by ~~an~~ authorized data ~~terminal~~ terminals ~~(T)~~[[.]];

[[-]] presenting the read secret code ~~(CODE)~~ to the user ~~(U)~~[[.]];

[[-]] ~~presenting a biometric feature (BIO) of a user~~ (U)[[.]] after receiving an indication that the presented read secret code is correct, reading a biometric feature presented by the user;

[[-]] comparing the presented biometric feature ~~(BIO)~~ with a biometric feature stored on the data carrier ~~(C)~~.

2. (Currently Amended) A method according to claim 1, ~~characterized in that~~ further comprising a step wherein a PIN is in addition presented to the terminal ~~(T), being~~ and compared with a PIN stored on the data carrier ~~(C)~~.

3. (Currently Amended) A method according to claim 1 or 2, ~~characterized in that~~ wherein a finger print of a user ~~(U)~~ is used as the biometric feature ~~(BIO)~~.

4. (Currently Amended) A data carrier ~~(C)~~ for authenticating a ~~terminal with respect to a user and the user with respect to~~ user of the data carrier for authorized use of the data carrier and for authenticating a data carrier terminal for accessing the data carrier, comprising a first memory area in which a secret code ~~(CODE)~~ is stored such that the secret code can be read and[[/or]] decrypted and displayed only by an authorized data

carrier terminal ~~(T)~~ to authenticate the data carrier terminal for accessing the data carrier, and a second memory area in which data are stored which serve to authenticate the user ~~with respect to the terminal~~ for authorized use of the data carrier.

5. (Currently Amended) A data carrier according to claim 4, ~~characterized in that~~ wherein a PIN is stored in a third memory area.

6. (Currently Amended) A data carrier according to either of claims 4 and 5, ~~characterized in that~~ wherein the biometric data are generated by a fingerprint.

7. (Currently Amended) An authentication system comprising a data carrier ~~(C)~~ with memory areas and a data carrier terminal ~~(T)~~ for accessing the memory areas of the data carrier, ~~characterized in that~~ wherein

[[-]] the data carrier ~~(C)~~ has a first memory area for storing a secret code ~~(CODE)~~ and a second memory area for storing biometric data,

[[-]] the data carrier terminal ~~(T)~~ has a first device which is authorized for reading the secret code ~~(CODE)~~ from the first memory area and[[/or]] for decrypting the read secret code ~~(CODE)~~ and for presenting the read secret code on a display, and a second device for reading biometric data ~~(BIO)~~ of a biometric feature presented by a user, and

[[-]] a device for comparing the read biometric data ~~(BIO)~~ with biometric data stored in the second memory area in the data carrier ~~(C)~~ and/or in the terminal ~~(T)~~.

8. (Currently Amended) An authentication system according to claim 7, ~~characterized in that~~ wherein the data carrier ~~(C)~~ has a third memory area for storing a PIN.

9. (Currently Amended) An authentication system according to claim 7 or 8, ~~characterized in that~~ wherein the stored biometric data are generated by a fingerprint.